TRICARE Management Activity Brown Bag Series 2004

Compliance through Risk Management

TMA Privacy Officer
TRICARE Management Activity
email: privacymail@tma.osd.mil

May 2004

Our Commitment to Security

The TRICARE Management Activity (TMA) Privacy Office is committed to ensuring the privacy and security of patient information at every level as we deliver the best medical care possible to those we serve.

TRICARE Management Activity

Presentation Objectives

- Explain implementation of HIPAA Security through organizational risk assessment
- Explain the role of the HIPAA Security Official
- Explain documentation requirements

What Is HIPAA?

Health Insurance Portability and Accountability Act (HIPAA)

Public Law 104-191 enacted August 21, 1996

- Improve portability & continuity of health insurance coverage
- Improve access to long term care services and coverage
- Simplify the administration of health care

Rule Background

Administrative Simplification Subtitle includes Four Rules

- Transactions and Code Sets
- Privacy
- Security
- Identifiers

Compliance Date for Security is April 21, 2005

What Information is Protected?

Electronic Protected Health Information (EPHI)

- Individually identifiable health information (including demographics) in electronic form
- Held by health plans, healthcare providers or their business associates

Any health information that identifies you as you and is in electronic form

Rule Objective

Implement reasonable and appropriate administrative, physical and technical safeguards to protect against any reasonably anticipated threats or hazards.

Rule Compliance

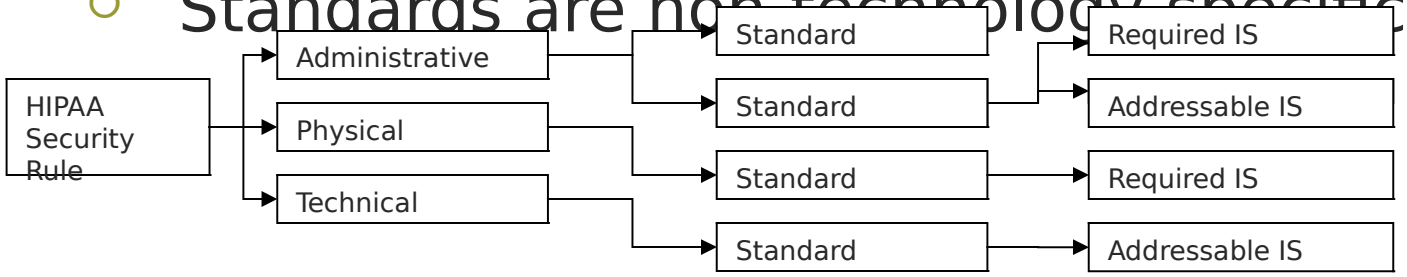
To correctly implement the security standards each covered entity must:

- Assess potential risks and vulnerabilities to EPHI;
- Develop, implement and maintain appropriate security measures given those risks; and
- Document those measures and keep them current

The key to compliance is Risk Management.

Rule Structure

- Organized into three categories; Administrative, Physical and Technical
- Categories contain standards and associated implementation specifications (IS)
  - All standards are required
  - IS may be either required or addressable
  - Standards are non-technology specific



What does “addressable” mean?

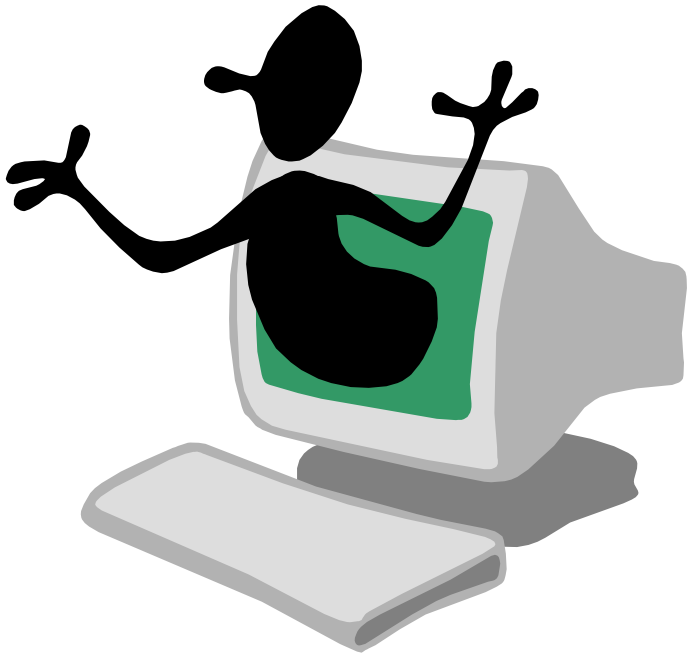
- Addressable IS must be assessed and reasonable and appropriate action taken based on results of:
  - Risk assessment
  - Mitigation strategy
  - Security measures already in place
  - Cost of alternatives
- Document action taken and rationale

The Decision Process

- If an addressable IS is determined to be:
  - Reasonable and appropriate, it must be implemented
  - Unreasonable or inappropriate, implement alternative safeguard that accomplishes same end
  - Not applicable or unreasonable/inappropriate and **standard** can be met without IS, implement only the standard
- Document action taken and rationale

What is Risk Management?

- Risk Management is composed of three parts
  - Risk Assessment
  - Risk Mitigation
  - Evaluation



Risk Assessment

- “Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by the covered entity.”
  - Must be organizational in nature – the whole picture
  - Identify the threats and vulnerabilities
  - Determine the impact of potential threats to assess risk
  - Identify safeguards in place that mitigate risk
  - Make recommendations to reduce residual risk

Risk Assessment Scope

- Determine the scope of the assessment
  - What is the asset
  - Why is it important
  - Describe the characteristics
  - Document

Threat Concepts

- Threat
  - Any circumstance or event with the potential to cause harm through unauthorized disclosure, unauthorized modification, or destruction of an asset
- Threat-Source
  - Threat-sources can be natural, environmental, or manmade
- Vulnerability
  - Weakness in a system or organization

Threats Exploit Vulnerabilities

Safeguards/Controls

- Best Practices
  - Safeguards and practices that mitigate threats
- Which are being done
- Which could be better
- Which are missing

Threat Impact

- Threat Outcomes
  - Unauthorized Disclosure
  - Unauthorized Modification
  - Unauthorized Destruction or Loss
  - Interruption or Denial of Access
- Impact on Organization
  - High, Medium or Low

Threats + Impact = Risk

Risk Assessment Methodology

- Provides a straightforward description of the system and a qualitative assessment of the risk (e.g., high, moderate, low)
- Risk assessment is composed of a nine-step systematic process
  1. Asset or System Characterization
  2. Threat Identification
  3. Vulnerability Identification
  4. Control Analysis
  5. Likelihood Determination
  6. Impact Analysis
  7. Risk Determination
  8. Control Recommendations
  9. Results Documentation

Risk Management

- “Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164-306(a)” [the rule objectives].
  - Identify additional safeguards to mitigate residual risks
  - Use the standards and IS as a guide
  - Create a plan to implement the safeguards and follow through
  - Document everything

Risk Mitigation

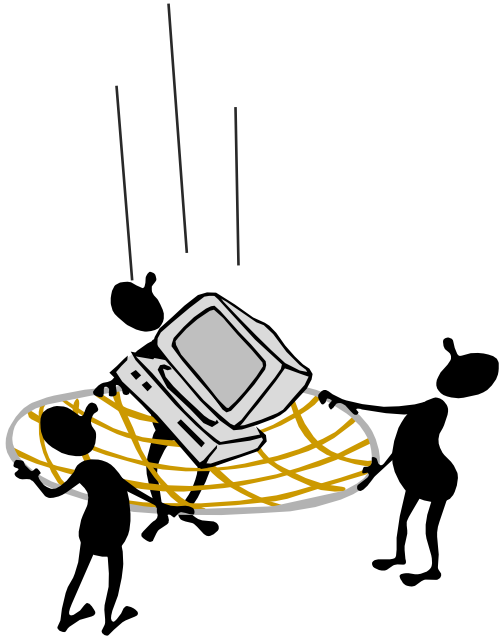
The process of identifying areas of risk that are unacceptable; and estimating countermeasures, costs and resources to be implemented as a measure to reduce the level of risk

Purpose

To enable management to make informed decisions regarding countermeasure analysis against known risk to a system(s)

Risk Mitigation

- Elimination of all risk is realistically impossible
- Management generally uses the most cost-effective approach and implements the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organization's resources and mission



Risk Mitigation Steps

- Step 1. Countermeasure Analysis & Expected Risk Reduction

- Step 2. Countermeasure Cost/Benefit Analysis

- Step 3. Monitor Performance

Rule Implementation

- Using the Security Rule requirements;
  - Conduct organizational risk assessment
  - Choose safeguards to mitigate risk
- Implement resulting risk management plan
- Document everything
- Review / Repeat

Diagram of Information Security Lifecycle

Corel – Policies, Standards and Guidelines

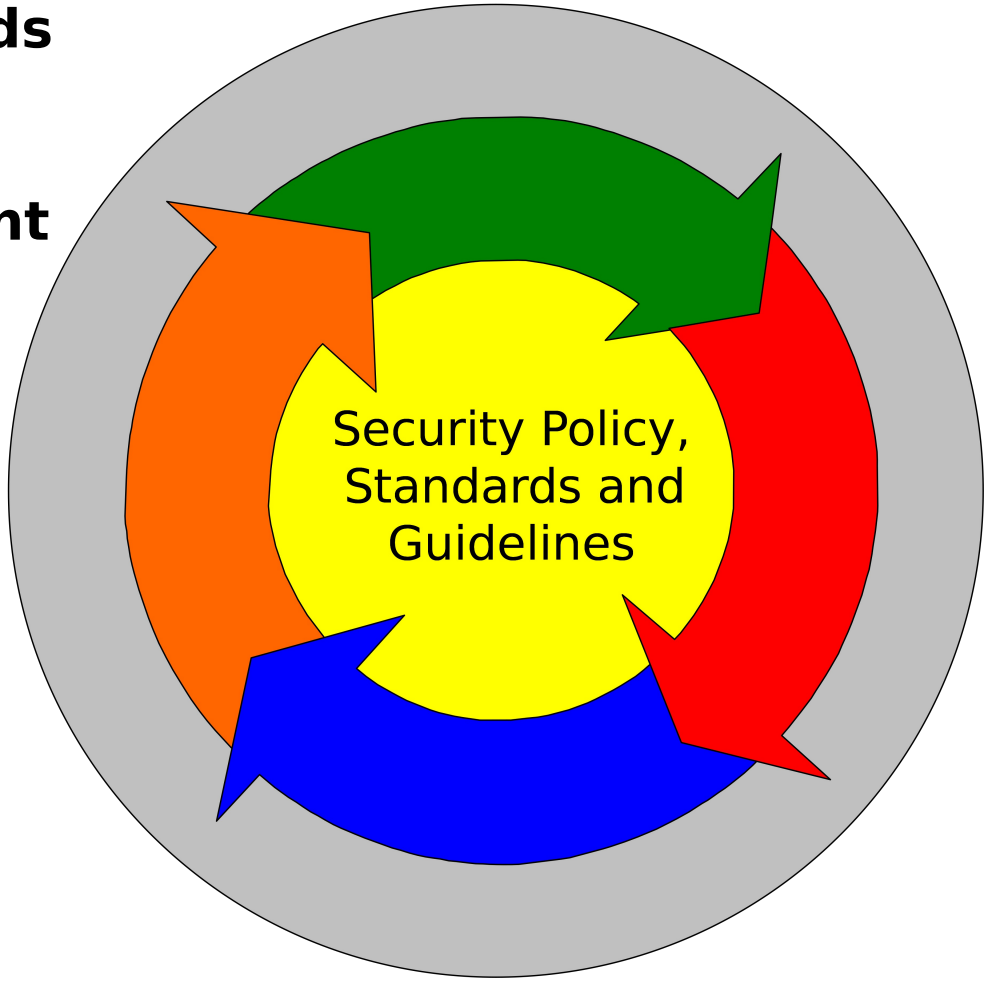
Conduct Risk Assessment

Perform Gap Analysis

Develop and Implement Mitigation Strategies

Sustainment and Maintenance

Continuous Education, Training and Awareness



HIPAA Security Officer

- “Identify the security official who is responsible for the development and implementation of the policies and procedures required by the HIPAA Security Rule.”
- Letters requiring appointment of HIPAA Security Officials in coordination for signature.

HIPAA Security Officer

- Areas of responsibility include:
  - Policy Implementation, Oversight, Auditing and Compliance
  - Education, Training and Communication
  - Administration of HIPAA Security Program
  - Liaison and Integration Activities

Documentation Requirements

- Maintain written policies and procedures
- Written record of all required actions, activities or assessments
  - Risk assessment, rationale for implementation of addressable IS, assignment of responsibility, evaluations, security incidents, business associate agreements
- Retain for 6 years
- Make available
- Review and update periodically

Documentation Tools

- Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE)
  - Process for conducting organizational risk assessment and development of risk management plan
  - Automated tool for documenting process and results
- HIPAA Basics
  - Compliance status tracking and reporting tool

HIPAA Security

Resources

- TMA HIPAA Web Site
  - **http://tricare.osd.mil/tmaprivacy/**
    - HIPAA Basics
    - Security module in HIPAA training tool
    - Information papers and FAQs
  - **privacymail@tma.osd.mil**
- RIMR - **https://rimr.tatrc.org/**
  - OCTAVE Implementation Guide
  - OCTAVE Automated Tool
  - P3WG Report

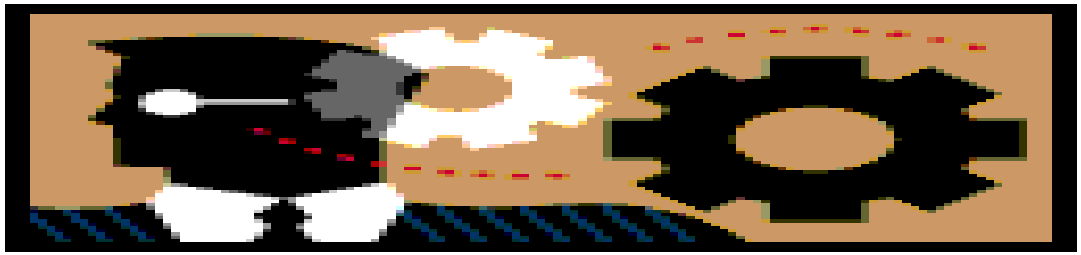
Our Commitment to Security

The TRICARE Management Activity (TMA) Privacy Office is committed to ensuring the privacy and security of patient information at every level as we deliver the best medical care possible to those we serve.

TRICARE Management Activity

QUESTIONS ?

QUESTIONS ?



QUESTIONS ?

QUESTIONS ?

QUESTIONS ?